09/937397 1C16 Rec'd PCT/PTO SEP 2 6 2001 SHEET 1 OF 1

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

ATTORNEY'S DKT No	APPLICATION NO.
032326-16	Unassigned
APPLICANT	· -
Jean-Sébastien CORON	
FILING DATE	GROUP
September 21, 2001	Unassigned

			U.S. PATENT DOCL	MENTS						
	U.S. Patent Document									
Examiner	Number	Kind Code	Name of Patentee or Applicant			Date of Publication				
Initials	Number	(if known)	of Cited D	(MM-DD-YYYY)						
· · · · ·		 								
								-		
			·							
		FC	REIGN PATENT DO	CUMENTS						
	Foreign Patent Document			_						
Examiner Initials	Number	Kind Code Number (if known) Country				ate of Publication (MM-DD-YYYY)	Translation Yes no			
			• • • • • • • • • • • • • • • • • • •							
	`						L	ļ		
										
							-			
			<u>-</u>				ļ	<u> </u>		
<u> </u>		<u> </u>					<u> </u>			
	<u></u>		ATENT LITERATUR					<u> </u>		
Examiner Initials	Include name of author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.									
NBC	Koblitz, Neal, "Elliptic Curve Cryptosystems", Mathematics of Computation, January 1987, Vol. 48, No. 177, pps. 203-209.									
NBP	Kocher, Paul, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", Advances In Cryptology, Crypto '96, Santa Barbara, Ca, USA, August 18-22, 1996, pps. 104-113.									
NBB	Kocher, Paul et al, "Introduction to Differential Power Analysis and Related Attacks", Cryptography Research, Inc., February 24, 2000, pps.1-8.									
nol	Menkus, Belden, Two Important Data Encryption Structures Reported Broken in Record Times", EDPACS, January 1999, Auerbach Publications, Vol. 26, No. 7, pps. 15-18.									
			·		_		<u>-</u> _	<u>. </u>		
	Ĭ									
Examiner Signature	Nov	~		Date Considered		8/15/05				

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP,609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. SEND TO: Assistant Commissioner for Patents, Washington, D.C. 20231.